Progetto S7/L5

Malware

Un malware e un exploit sono concetti distinti nel campo della sicurezza informatica. Il malware è un software dannoso progettato per infiltrarsi o danneggiare un sistema, spesso senza il consenso dell'utente. Esistono diverse categorie di malware, ognuna con uno scopo specifico. Ad esempio, i virus infettano altri file o programmi, i worm si diffondono autonomamente attraverso le reti, mentre i ransomware crittografano i dati chiedendo un riscatto per ripristinarli, e così via.

Exploit

Gli exploit, d'altra parte, sono specifici metodi o codici che sfruttano le vulnerabilità di un sistema o di un'applicazione. Le vulnerabilità possono derivare da errori di programmazione, falle di sicurezza o problemi di progettazione che permettono agli hacker di ottenere accesso non autorizzato o eseguire codice malevolo. Gli exploit possono essere utilizzati per sfruttare queste vulnerabilità e introdurre malware nei sistemi bersaglio. Spesso vengono descritti con riferimento alle vulnerabilità specifiche che sfruttano, come **"exploit di buffer overflow"**.

In sostanza, il malware causa danni, mentre gli exploit sono gli strumenti che ne rendono possibile l'esecuzione.

Metasploit

Metasploit è un framework di test di penetrazione open-source utilizzato dagli esperti di sicurezza informatica per sviluppare, testare e eseguire exploit su sistemi informatici al fine di identificare vulnerabilità. Fondato su un vasto database di exploit e payload, Metasploit fornisce una piattaforma versatile per testare la sicurezza di reti e sistemi. È stato creato con l'obiettivo di educare sulla sicurezza informatica e facilitare la ricerca sulle vulnerabilità.

Meterpreter

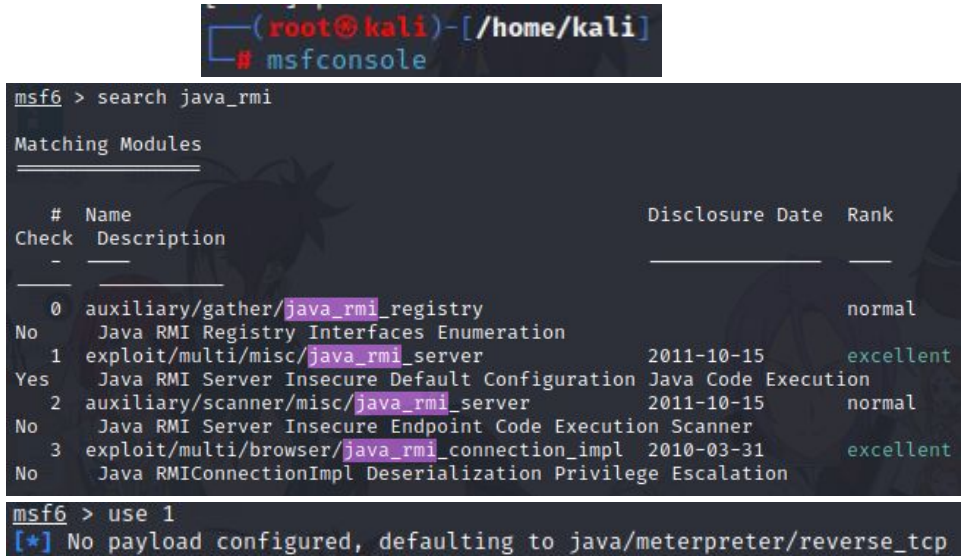
Meterpreter, d'altra parte, è un payload di Metasploit progettato per fornire una vasta gamma di funzionalità durante le operazioni di test di penetrazione. Funziona come un interprete di comandi da remoto, consentendo agli utenti di eseguire comandi sul sistema bersaglio, acquisire informazioni, avviare processi, catturare schermate e molto altro. È una componente fondamentale per gli hacker etici impegnati in test di sicurezza.

Esercizio

Parliamo del servizio di cui stiamo sfruttando la vulnerabilità. Java Remote Method Invocation (RMI) è un meccanismo di comunicazione tra processi in ambiente Java. Consente a un'applicazione Java su una macchina virtuale di chiamare metodi di oggetti su un'altra macchina virtuale, facilitando la comunicazione distribuita. La porta 1099 è comunemente utilizzata per registrare e cercare servizi RMI attraverso il registry RMI.

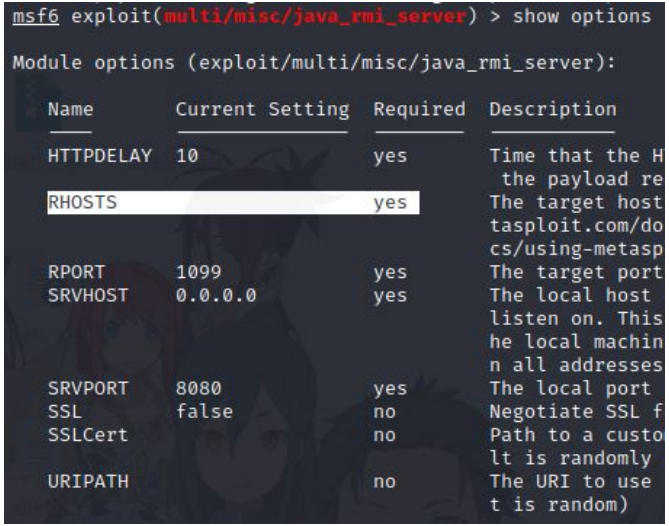
Esercizio

Dopo aver cambiato gli indirizzi IP ed aver controllato le porte aperte con nmap, apriamo un terminale, eseguiamo msfconsole e successivamente eseguiamo una ricerca con il comando search java_rmi. Nella pratica corretta, è consigliato controllare tutte le vulnerabilità, ma nel nostro caso stiamo seguendo una specifica traccia e ci concentreremo solo sull'exploit exploit/multi/misc/java_rmi_server.



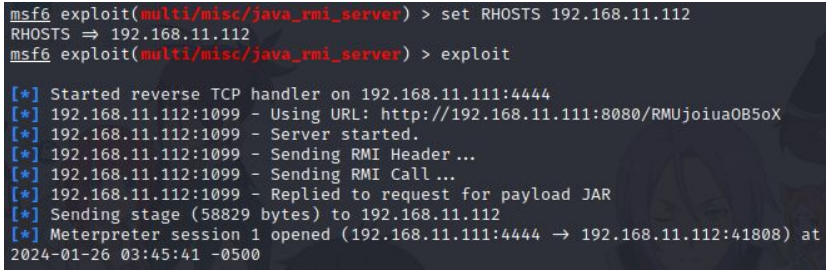
Esercizio

Inseriamo show options per visualizzare i cambiamenti fondamentali da apportare. Secondo la traccia, se la macchina restituisce un errore, è necessario modificare anche HTTPDELAY a 20. Nel mio caso, modifico solamente RHOSTS con l'indirizzo IP 192.168.11.112.



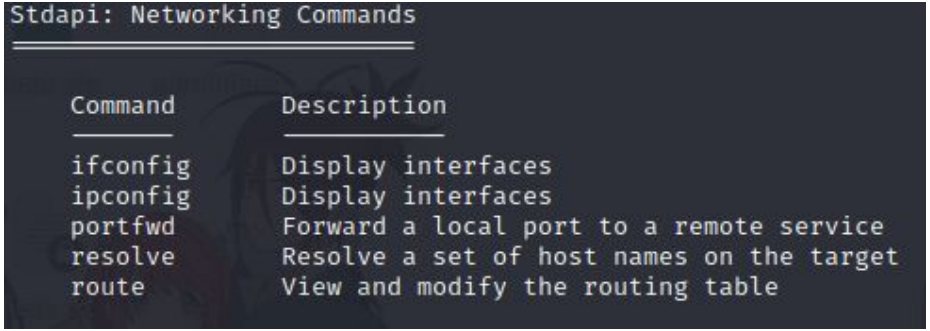
Esercizio

Ora che abbiamo impostato l'IP della macchina vittima, eseguiamo exploit. Dall'ultimo messaggio, comprendiamo che una sessione di Meterpreter è stata aperta.



Esercizio

Ipotizziamo di non conoscere i comandi di Meterpreter. Ho utilizzato il comando help per trovare le informazioni necessarie. Ora possiamo visualizzare sia la configurazione di rete che le informazioni sulla tabella di routing della macchina vittima.



Esercizio

Ecco qui a destra la configurazione di rete.

Esercizio

Ecco qui a destra le informazioni sulla tabella di routing della macchina vittima.